



Office of Security

National Security Information On-Line Refresher Briefing

2007



SF-312 Nondisclosure Agreement

- A binding contract with the U.S. Government
- Lifetime obligation to protect and never disclose classified
- Enables you to get access to classified

CLASSIFIED INFORMATION NONDISCLOSURE AGREEMENT

AN AGREEMENT BETWEEN
STATES

AND THE UNITED
STATES

(Name of Individual - Printed or typed)

I, intending to be legally bound, hereby accept the obligations contained in this Agreement in consideration of my being granted access to classified information. As used in this Agreement, classified information is marked or unmarked classified information, including oral communications, that is classified under the standards of Executive Order 12958, or under any other Executive order or statute that prohibits the unauthorized disclosure of information in the interest of national security, and unclassified information that meets the standards for classification and is in the process of a classification determination as provided in Sections 1.1, 1.2, 1.3 and 1.4(c) of Executive Order 12958, or under any other Executive order or statute that requires protection for such information in the interest of national security. I understand and accept that by being granted access to classified information, special confidence and trust shall be placed in me by the United States Government.

2. I hereby acknowledge that I have received a security indoctrination concerning the nature and protection of classified information, including the procedures to be followed in ascertaining whether other persons to whom I contemplate disclosing this information have been approved for access to it, and that I understand these procedures.

3. I have been advised that the unauthorized disclosure, unauthorized retention, or negligent handling of classified information by me could cause damage or irreparable injury to the United States or could be used to advantage by a foreign nation. I hereby agree that I will never divulge classified information to anyone unless: (a) I have officially verified that the recipient has been properly authorized by the United States Government to receive it; or (b) I have been given prior written notice of authorization from the United States Government Department or Agency (hereinafter Department or Agency) responsible for the classification of information or last granting me a security clearance that such disclosure is permitted. I understand that if I am uncertain about the classification status of information, I am required to confirm from an authorized official that the information is unclassified before I may disclose it, except to a person as provided in (a) or (b), above. I further understand that I am obligated to comply with laws and regulations that prohibit the unauthorized disclosure of classified information.

4. I have been advised that any breach of this Agreement may result in the termination of any security clearances I hold; removal from any position of special confidence and trust requiring such clearances; or termination of my employment or other relationships with the Departments or Agencies that granted my security clearance or clearances. In addition, I have been advised that any unauthorized disclosure of classified information by me may constitute a violation, or violations, of United States criminal laws, including the provisions of Sections 641, 793, 794, 798, *952 and 1924, Title 18, United States Code, *the provisions of Section 783(b), Title 50, United States Code, and the provisions of the Intelligence Identities Protection Act of 1982. I recognize that nothing in this Agreement constitutes a waiver by the United States of the right to prosecute me for any statutory violation.

5. I hereby assign to the United States Government all royalties, remunerations, and emoluments that have resulted, will result or may result from any disclosure, publication or revelation of classified information not consistent with the terms of this Agreement.

6. I understand that the United States Government may seek any remedy available to it to enforce this Agreement including, but not limited to, application for a court order prohibiting disclosure of information in breach of this Agreement.

7. I understand that all classified information to which I have access or may obtain access by signing this Agreement is now and will remain the property of, or under the control of the United States Government unless and until otherwise determined by an authorized official or final ruling of a court of law. I agree that I shall return all classified materials which have, or may come into my possession or for which I am responsible because of such access: (a) upon demand by an authorized representative of the United States Government; (b) upon the conclusion of my employment or other relationship with the Department or Agency that last granted me a security clearance or that provided me access to classified information; or (c)

Unauthorized Disclosure of National Security Information

- **Security Infraction**: occurs when classified information is not safeguarded but does not result in a compromise of material
- **Security Violation**: occurs when classified information is not safeguarded and could result in a probable compromise of material
- **Compromise**: an actual compromise of classified information, whether intentional or unintentional



Penalties for Compromising Classified Information (Executive Order 12958)

- Reprimand,
- Suspension without pay,
- Denial of future access,
- Removal from position, and/or
- Criminal prosecutions



Levels of Classified Information

There are three levels of classified information:



It is a good security practice use cover sheets on classified information!

Original vs. Derivative Classification

Original

- **Classified by:** OCA name and title
- **Reason:** from section 1.4 (a-h), E.O. 12958, as amended
- **Declassify on:** within 25 years from original date
- Need written authority

Derivative

- Incorporates, restates, or paraphrases from source document or classification guide
- **Derived from:** source or classification guide
- **Declassify on:** from source or guide
- No written authority needed

Derivative Classifications & Prohibited Classification Markings

- Since Sep 22, 2003, use of X1 through X8 exemptions on newly created documents is prohibited and has caused confusion and ambiguity as to the duration of the classification.
- Henceforth, if you create a new derivative document from a classified source document that is dated after Sep 22, 2003, and it uses X1 thru X8 on the “Declassify On” line, you must mark the “Declassify On” line with “September 22, 2028” date on your newly created derivative document.
- This guidance is intended to remove ambiguity and is effective immediately. (Source: ISOO memo, 16 Feb 07)

Classified Information Properly Marked

Paragraph/
Portion Markings

SECRET

Overall Classification
Marking

This memo is for training purposes only (U)

(U) This paragraph contains unclassified information

(S) This paragraph contains secret information relating to U.S. National Security

(U) This paragraph contains unclassified information

Classified By: Jane Till, Deputy Under Secretary for Economic Affairs

Classify
By line or
Derive
From line

Reason: 1.4 (e) through (h)

Reason Line

Declassify on: 13 December 2009

Declassification Date

SECRET

Overall Classification
Marking

Declassification

- Documents are generally marked for declassification 10-25 years from the original date of document
- Only an Original Classification Authority can authorize declassification
- If the “Declassify On” line date has passed on a classified document, custodians should refer the document to the originating agency to ensure the declassification date has not been extended

Sensitive Information



Information marked “Sensitive,” “For Official Use Only,” “Sensitive But Unclassified,” “Company Proprietary,” etc., is **not** classified.

However, protection from unauthorized disclosure is still required.

Remember sensitive information should not be marked with classified markings (Top Secret, Secret, Confidential).

Accountability of Classified Information

- All persons who handle classified information are personally accountable for the protection and control of this information.
- You must limit access to authorized persons by **verifying**:
 - **Identification-** *does the person have valid identification?*
 - **Need to know-** *does the person have a “need to know” in order to perform their job?*
 - **Clearance-** *does the person have the appropriate security clearance? When in doubt, verify with your servicing security office*
 - **Ability to protect-** *does the person have the ability to protect, for example, have approved storage capabilities?*

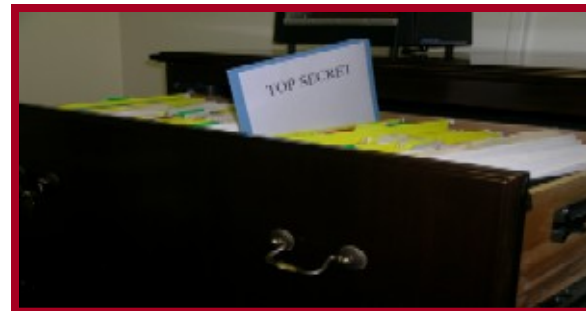
Protecting Classified



Classified information must be stored in a GSA-approved security container (safe) when not in use

DO NOT STORE CLASSIFIED IN THE FOLLOWING:

- Desk Drawers
- Filing Cabinets
- Overhead Cabinets
- Window Sills



Safe Combinations

- Security container combinations are classified at the level of information stored in the safe
- Memorize combinations—never write them down

Change combinations when...

- Security container is found open
- Someone who has the combination leaves the office (update form SF-700, Security Container Information)
- Security container is surplus

Marking Classified Information: Electronic Media

Removable storage media and devices such as diskettes, CD-ROMS, video cassettes, etc., must have an outer label with the classified markings affixed.



Protecting Classified

NO unauthorized use of computers!

- Do not generate classified information on any computer system unless approved for classified usage
- See your Bureau Information Technology Security Officer

Transmitting Classified Telephone/Fax

- Always use a STU-III or STE telephone for classified telephone conversations
- Use compatible, cleared facsimile machines for quick and secure classified document transmission



Transporting Classified

Within a Facility

- Classified information hand-carried between offices must be shielded by the appropriate cover sheet to prevent disclosure
- Employees transporting classified within a facility should not carry classified into public areas (e.g., cafeteria, bathroom, etc.) while en route to their destination



Transporting Classified Mail/Courier

Secret and Confidential may be transported by the following means:

- Hand-carry
- United States Postal Service
 - (Secret: Registered, Confidential: Certified or 1st Class)
- Approved classified courier

To transport Top Secret, in any manner, call your security officer



Transporting : Double-wrapping

Mail/Courier

- Must be done to prepare for hand-carry or send via U.S. Postal Service
- Affords 2 layers of protection - use opaque envelopes
- Don't forget to include a receipt
- **Inner wrapping**
 - Includes full address, agency/office (with individual's name)
 - Your return address
 - Classification markings
 - Receipt
- **Outer wrapping**
 - Includes full address, agency/office (**do not** include individual's name)
 - Your return address
 - **NO CLASSIFICATION MARKINGS ON OUTER WRAPPING**



Reproduction of Classified

- Verify photocopier is approved for classified usage

Approved photocopiers are:

- In controlled environments
 - Sanitized after classified copying
 - Serviced by cleared or monitored personnel
- Contact servicing security office for approval



Classified Destruction

- Shredding

- GSA approved cross-cut shredder that renders the material 1/32" in width and 3/8" in length



- Classified waste “burn bags”

- Must be protected in approved storage container until destroyed!

For additional classified destruction information, contact your servicing security officer

Most classified leaks result from:

- Negligence
- Carelessness
- Casual Conversations
- Open Sources



Reporting Requirements

All cleared employees must report contact with anyone who:

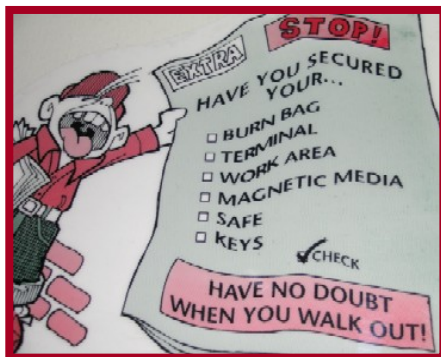
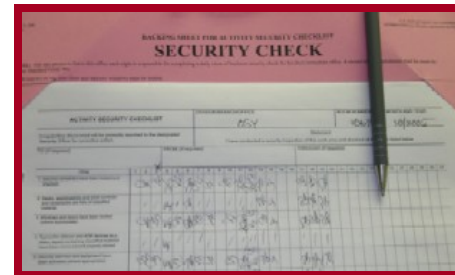
- Suspiciously requests classified information
- Acts suspiciously
- Wants more information than they need to know

Report incidents to your security officer immediately!



End-of-Day Security Checks

- Check all areas to include safes, windows, desktops for classified
- Complete the SF-701, Activity Security Checklist



- Complete SF-702, Security Container Checklist
- Turn on alarm, if appropriate

Your Security Officer

- Be **PROACTIVE**
- Request help
- Report
 - Security violations
 - Suspected loss or compromise
 - Incidents or problems

